

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) Computer apparatus, comprising:
a receiver for receiving an integrity metric for a computer entity via a trusted device associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer entity; and
a controller for assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric.
2. (original) Computer apparatus according to claim 1, wherein the trusted device is arranged to acquire an integrity metric of the computer entity.
3. (original) Computer apparatus according to claim 1, wherein the trust level is determined by comparing the value of the at least one characteristics with a specified value.
4. (original) Computer apparatus according to claim 1, wherein the plurality of trust levels are determined base upon a plurality of specified values associated with a plurality of characteristics of a computer entity.
5. (original) Computer apparatus according to claim 1, wherein the plurality of trust levels are determined based upon a plurality of specified values associated with characteristics

for a plurality of computer entities.

6. (currently amended) A method of assigning a trust level,
~~the method comprising:~~

receiving an integrity metric for a computer entity via a
trusted device associated with the computer entity, the
integrity metric having values for a plurality of
characteristics associated with the computer entity; and

assigning a trust level to the computer entity from a
plurality of trust levels, wherein the assigned trust level is
based upon the value of at least one of the characteristics of
the received integrity metric.

7. (New) A method for establishing communications with a
computer entity, comprising:

requesting a trusted device associated with a computer
entity to provide an integrity metric calculated for the entity
by the trusted device and containing values indicative of one or
more characteristics of the entity;

receiving a response from the trusted device including an
integrity metric calculated for the entity by the trusted
device;

comparing values in the integrity metric calculated for the
entity by the trusted device with authenticated values provided
for the entity by a trusted party; and

selecting a level of trust for the entity from a plurality
of predefined levels of trusts based on at least one value in
the integrity metric calculated for the entity by the trusted
device.

8. (New) The method of claim 7, wherein the trusted device

is hardwired to the computer entity.

9. (New) The method of claim 8, wherein the trusted device is configured to control the boot process of the computer entity.

10. (New) The method of claim 9, wherein the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

11. (New) The method of claim 8, wherein the trusted device is comprised of a plurality of components hardwired to the computer entity.

12. (New) The method of claim 7, wherein the trusted device is configured to contain one or more of a public encryption key, a private encryption key, and one or more authenticated values provided for the entity integrity metric by the trusted party.

13. (New) The method of claim 12, wherein the trusted device is configured to calculate the integrity metric by generating a digest of BIOS instructions in the BIOS memory of the entity.

14. (New) The method of claim 12, wherein the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity.

15. (New) The method of claim 14, wherein the components of

the entity are selected from among the group of components comprising hardware components and software components.

16. (New) The method of claim 15, wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity.

17. (New) The method of claim 15, wherein the configuration information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous update information.

18. (New) The method of claim 12, wherein the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components.

19. (New) The method of claim 12, wherein the response received from the trusted device includes the authenticated values provided by the trusted party.

20. (New) The method of claim 7, wherein requesting the trusted device for the integrity metric comprises:

generating a nonce to pass to the trusted device with the request.

21. (New) The method of claim 20, wherein the response from the trusted device includes the nonce received with the request.

22. (New) The method of claim 7, further comprising:
initiating data transfer to the entity in accordance with
the selected trust level.

23. (New) The method of claim 22, wherein initiating data
transfer to the entity in accordance with the selected trust
level comprises transferring no data.

24. (New) A method for a computer entity to respond to a
request for integrity check prior to exchanging data,
comprising:

receiving at a trusted device associated with a computer
entity a request to provide an integrity metric containing
values indicative of one or more characteristics of the entity;
calculating at the trusted device values indicative of one
or more characteristics of the entity; and
providing a response from the trusted device including an
integrity metric including the values indicative of one or more
characteristics of the entity.

25. (New) The method of claim 24, wherein the trusted
device is hardwired to the computer entity.

26. (New) The method of claim 25, wherein the trusted
device is configured to control the boot process of the computer
entity.

27. (New) The method of claim 25, wherein the trusted
device is configured to not respond to the request for the
integrity metric if the boot process of the computer entity was

not controlled by the trusted device.

28. (New) The method of claim 25, wherein the trusted device is comprised of a plurality of components hardwired to the computer entity.

29. (New) The method of claim 24, wherein the trusted device is configured to contain one or more of a public encryption key, a private encryption key, and one or more authenticated values provided for the entity integrity metric by the trusted party.

30. (New) The method of claim 29, wherein the integrity metric includes one or more values calculated by generating a digest of BIOS instructions in the BIOS memory of the entity.

31. (New) The method of claim 29, wherein the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity.

32. (New) The method of claim 31, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

33. (New) The method of claim 32, wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity.

34. (New) The method of claim 32, wherein the configuration

information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous update information.

35. (New) The method of claim 29, wherein the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components.

36. (New) The method of claim 35, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

37. (New) The method of claim 29, wherein the response further includes authenticated values provided for the entity by a trusted party.

38. (New) The method of claim 29, wherein the request includes a nonce.

39. (New) The method of claim 38, wherein the response includes the nonce received with the request.

40. (New) The method of claim 29, wherein the request includes input data.

41. (New) The method of claim 40, wherein the response includes the input data processed with the private encryption key.

42. A method for establishing communications between a computer entity and a user, comprising:

presenting a request from the user to a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity;

presenting to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device;

comparing at the user values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party; and

selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user based on at least one value in the integrity metric calculated for the entity by the trusted device.

43. (New) The method of claim 42, wherein the trusted device is hardwired to the computer entity.

44. (New) The method of claim 43, wherein the trusted device is configured to control the boot process of the computer entity.

45. (New) The method of claim 44, wherein the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

46. (New) The method of claim 43, wherein the trusted device is comprised of a plurality of components hardwired to the computer entity.

47. (New) The method of claim 42, further comprising: passing from the trusted party to the trusted device one or more of a public encryption key, a private encryption key, and one or more authenticated values for the entity integrity metric.

48. (New) The method of claim 47, wherein the trusted device is configured to calculate the integrity metric by generating a digest of BIOS instructions in the BIOS memory of the entity.

49. (New) The method of claim 47, wherein the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity.

50. (New) The method of claim 49, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

51. (New) The method of claim 50, wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity.

52. (New) The method of claim 50, wherein the configuration information measured for at least one of the components comprises one or more of certificate information, last update

information, latest update version information, and previous update information.

53. (New) The method of claim 47, wherein the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components.

54. (New) The method of claim 49, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

55. (New) The method of claim 47, wherein the response received from the trusted device includes the authenticated values provided by the trusted party.

56. (New) The method of claim 42, wherein the request includes a nonce.

57. (New) The method of claim 56, wherein the response includes the nonce received with the request.

58. (New) The method of claim 47, wherein the request includes input data.

59. (New) The method of claim 58, wherein the response includes the input data processed with the private encryption key.

60. (New) The method of claim 42, further comprising:

initiating data transfer from the user to the entity in accordance with the selected trust level.

61. (New) The method of claim 60, wherein initiating data transfer from the user to the entity in accordance with the selected trust level comprises transferring no data.